Mist Integration with ISE for Guest Access

Table of Contents

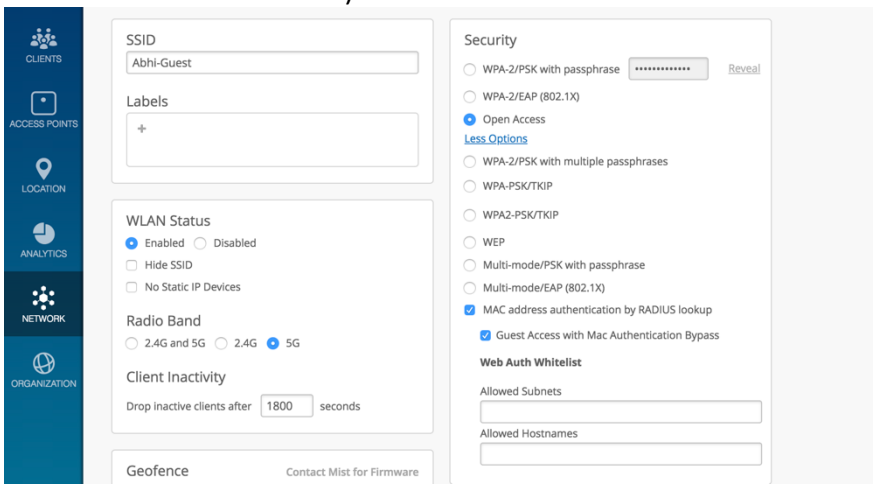
Flow of Guest Access via Radius Server using MAB

1) Wireless MAB WLAN is created on the Mist AP with MAB being performed via Radius Lookup.
2) When a client associated to this WLAN, the the mac address of the client is sent across to the radius server via an ACCESS_REQUEST
3) Radius server looks up its database and if the client is not found in the database, sends back a ACCESS_ACCEPT with a redirection URL to the Mist AP
4) The client now is provided with limited access to the network which includes access to the BOOTP, DNS and Radius server
5) After the client receives an IP, the AP opens a web socket to and listens to any HTTP traffic initiated from the client
6) Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
7) The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
8) Once the client provides necessary info on the URL, the ISE now install this client's mac address in its database and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.
9) The Mist AP upon receiving the CoA request – acknowledges the request and sends back the same ACCESS_REQUEST as in step 2.
10) At this point - the client is available in the radius server database and hence would be provided with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined.

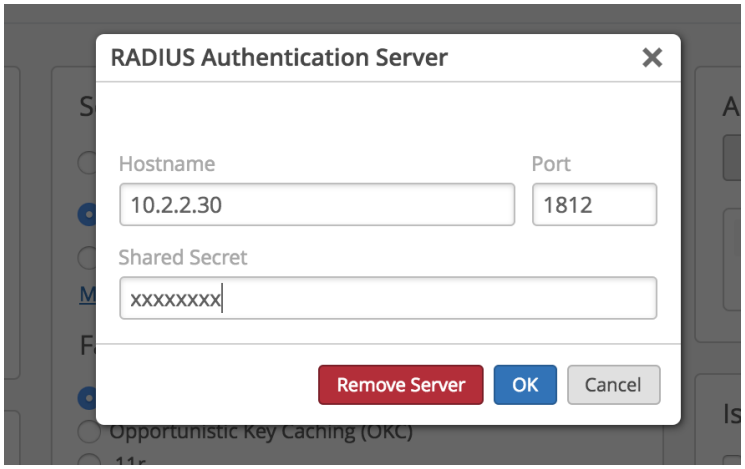
Mist AP Configuration

WLAN Configuration

a. Network -> WLAN -> Add WLANs
b. Enable “MAB by Radius lookup” and “Guest Access with MAB” under it
c. You can use the Whitelist in order to permit specific subnets/hostnames when the client is in the redirect state (It is optional – if left blank, the radius server is the only IP that is whitelisted for access)

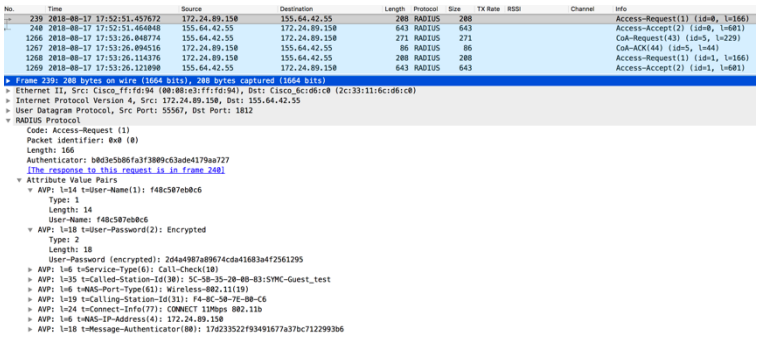


d. Add the Radius Server of Choice (RadSec is disabled when not used)
   i. Click on the Radius server and it will provide an option to input the Radius Server details (IP, Port, Shared Secret) which would be the Radius server IP and port details
   ii. You would also have the option of adding a secondary-server/tertiary servers
   iii. You will also be edit the order of the preference for servers using the arrow keys place beside them.

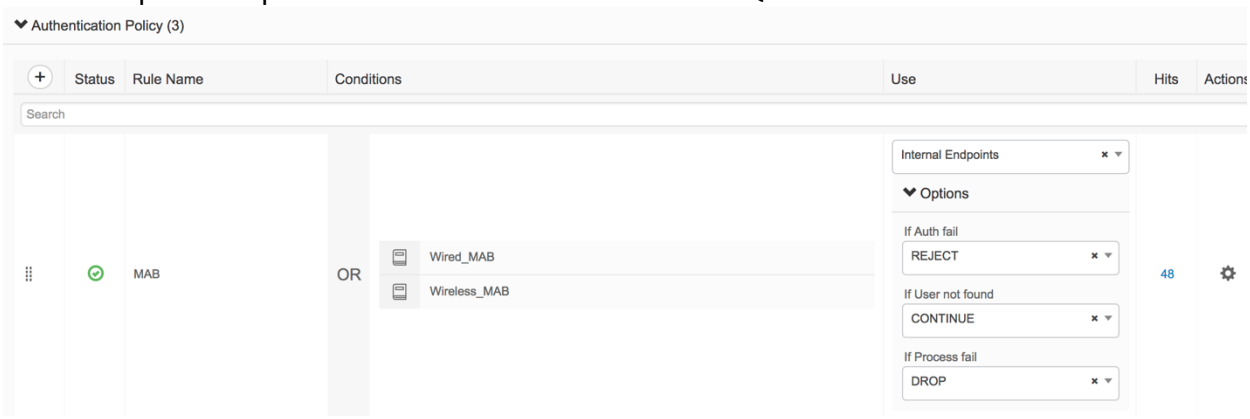


Authentication Policy

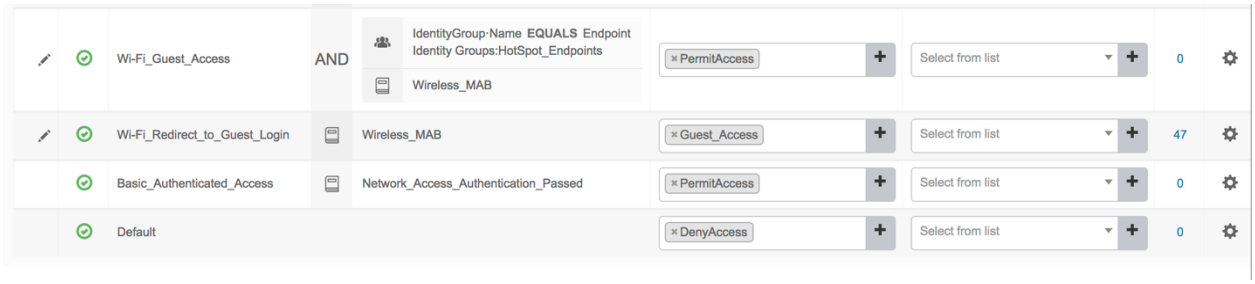
a. When a client associates to this WLAN, the access point sends a ACCESS-REQUEST to Radius Server



b. The packet capture above indicates the ACCESS-REQUEST sent across from the client



c. The authentication policy on the radius server is tailored to “continue” if the user is not found in the database. This allows the client to get an IP and be placed in the redirect state.

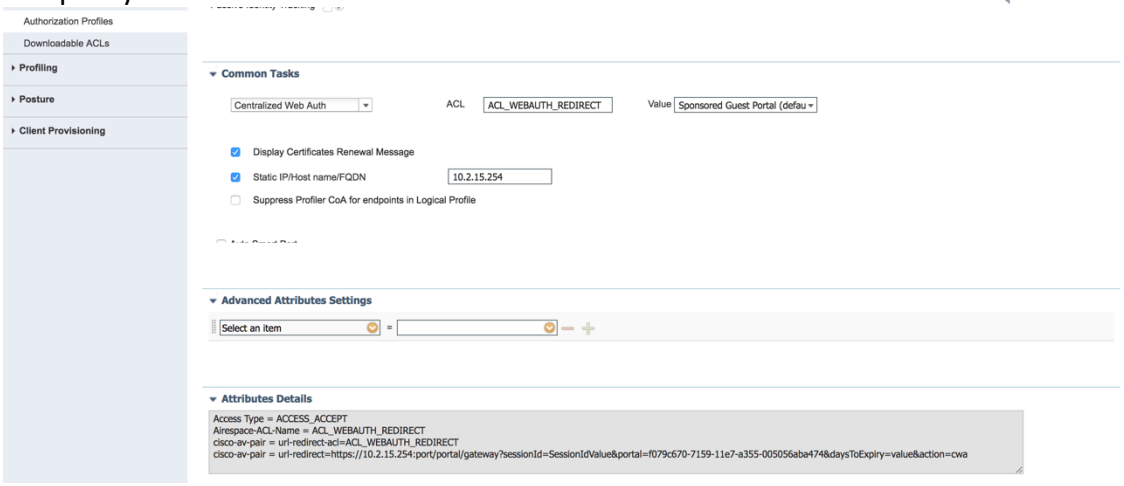


d. The authorization policy has two policies that will be hit during the process of this guest access flow. The first policy that is hit as indicated above is “Wifi_Redirect_to_Guest_Login” which provides partial access to the client.

   i. Note: Upon successful auth after CoA we hit the second auth indicated as “Wifi_Guest_Access” which provides full access to the client

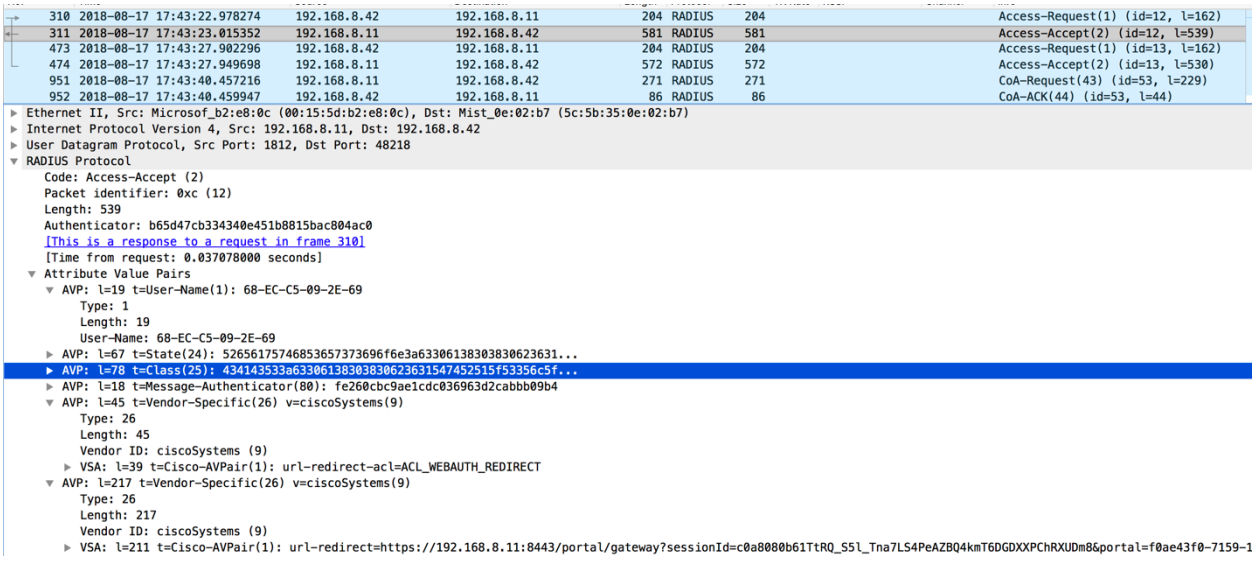
Authorization Profile

Once we hit the first policy MAB policy on the Radius server, the server responds with an Access-Accept to the Mist AP but also provides a redirect URL which is presented to the client. The policy is created as below in the radius server



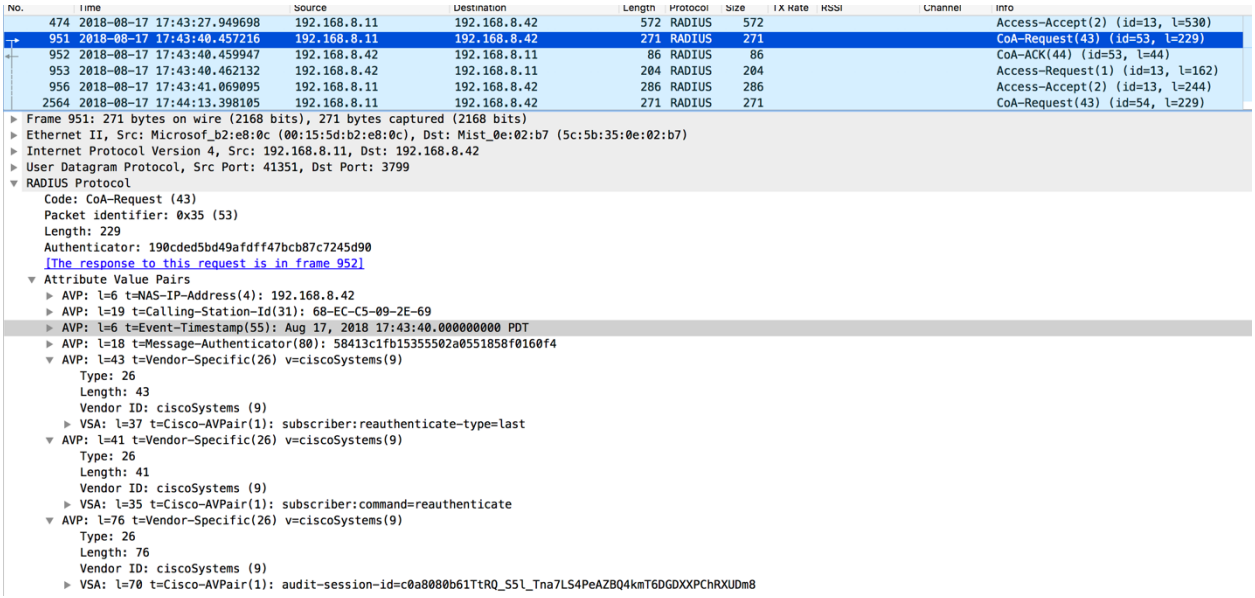
The Radius server response would contain the above URL as shown in the packet capture below.

Note: Although there is an ACL that is presented as well as a part of the response, at Mist, we wouldn't need to configure any ACL/WxLAN policies as the we have a built in wall garden policy which provide BOOTP, DNS and ISE server access only to the client.



URL redirect

- At this stage, client is able to procure an IP.
- The client should initiate an HTTP transaction – by logging into the browser and trying to reach an external URL
- Any HTTP traffic initiated from the client is intercepted and is responded with a URL that was sent by Radius server
- The client is presented with URL. Based on the policy: it might be a sponsored portal, a self registration portal or a hotspot portal.
- Once the client provides necessary info on the URL, **the radius server now installs this client's mac address in its database** and also issues a CoA (Change of Authorization) request with a command to re-authorize this client.

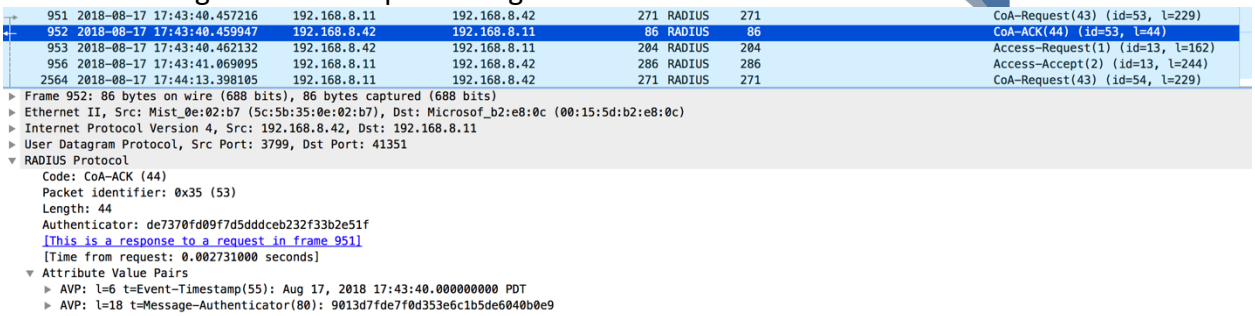


Note:

1) The key observation in the CoA request is that Cisco AV pair Subscriber:Command has the value "reauthenticate". This is the reason why we are able to authorize a client for the second time around without having to disconnect the client.
2) The Cisco AV pair Subscriber:Reauthenticate-type has the value "last" which indicates that the Mist AP should use the same access request as it presented the last time for the client in question.

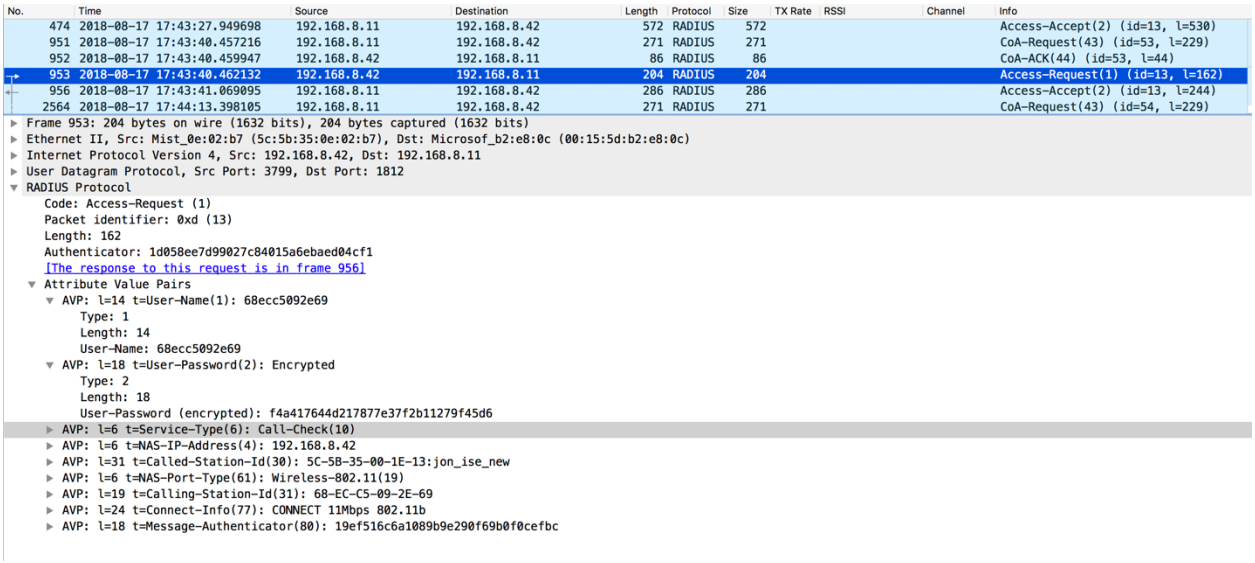
CoA(Change of Authorization)

We acknowledge this CoA request using a CoA Ack

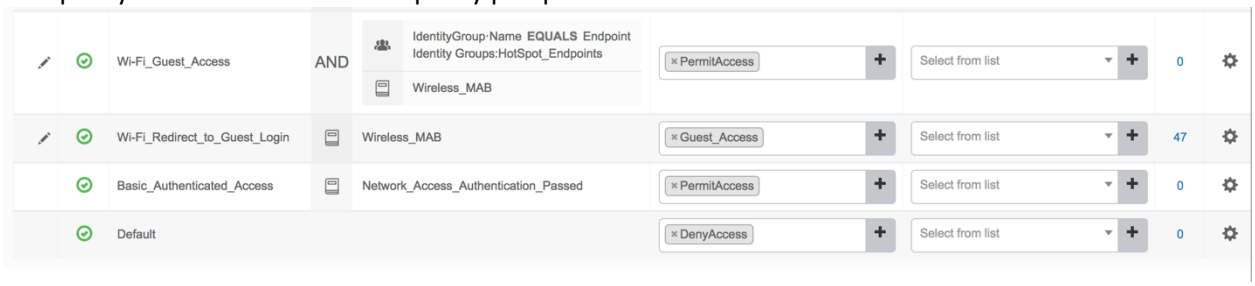


Second Access Request and Permit Access

- Based on the CoA request – we send the same ACCESS REQUEST back to the client



- At this point - the client is available in the radius server database and hence we hit the second policy from the authorization policy perspective.



In the above example – we would meet the criteria for the policy named “Wifi_Guest_Access” since the hotspot clients are stored in the Hotspot_Endpoints Identity Group. Hence the client would be provided

with a ACCESS-ACCEPT without any restrictions of URL-Redirect and the client would have network connectivity based on the policies defined which in this case is “PermitAccess”